NCOIC GEOINT Community Cloud

John Pritchard, IBM

Kevin Jackson, NJVC

Mark Reichardt

This document does not contain technical data within the definition contained in the International Traffic in Arms Regulations (ITAR) and the Export Administration Regulations (EAR), as such is releasable by any means to any person whether in the U. S. or abroad. The Export Compliance log number for this document is [Export Approval # JLT2250-NT (assigned IAW PRO-4527,PRO 3439).

Sharing Geospatial Intelligence and Services

David L. Bottom
Director ISP Core Services Office
David.L.Bottom@nga.mil
301-227-0992

Approved for Public Release 10-328

Addressing the Problem

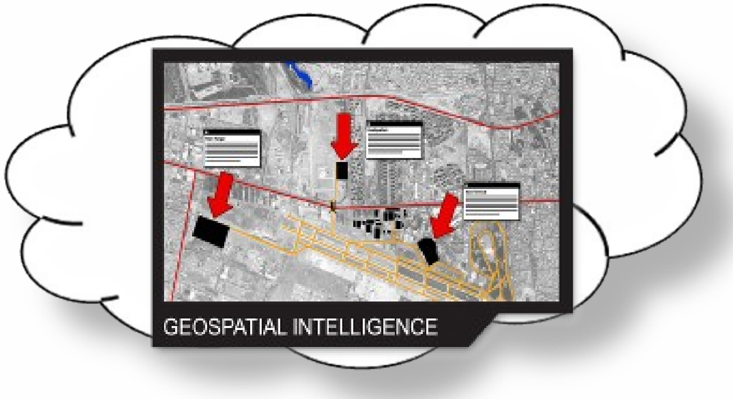
Mission

Data

Systems

Standards

CLOUD?



Optimizing GEOINT Sharing and Exchange

Geospatial Community Cloud Project

- Establish standards and processes necessary to enable a global Geospatial Community Cloud
    - Address issues associated with compatibility, speed of access and data protection

- Maximize the use of industry open standards and best practices
    - Utilize NCOIC Integrated Product Teams

- Design to operate within processes and procedures NATO developing for electronic dissemination of geospatial data

- Enable Fighting off the Same Map

Next Steps

- NCOIC members provide recommendations
- NGA assess systems for inclusion in NCOIC Test Bed
- NGA brief NATO Geospatial Conference (30 June 10)
- Brief Plan of Action and Milestones at next NCOIC Plenary (Sept 10)

Potential Areas for NCOIC to Address

- **How do we leverage industry best practices to globally provide access to electronic GEOINT data and services**

- **How can we protect digital GEOINT data from unauthorized use while maintaining the ability of each participating country to manage the data that they provide?**

- **How can GEOINT data and services be provided and consumed within a bandwidth challenged environment?**

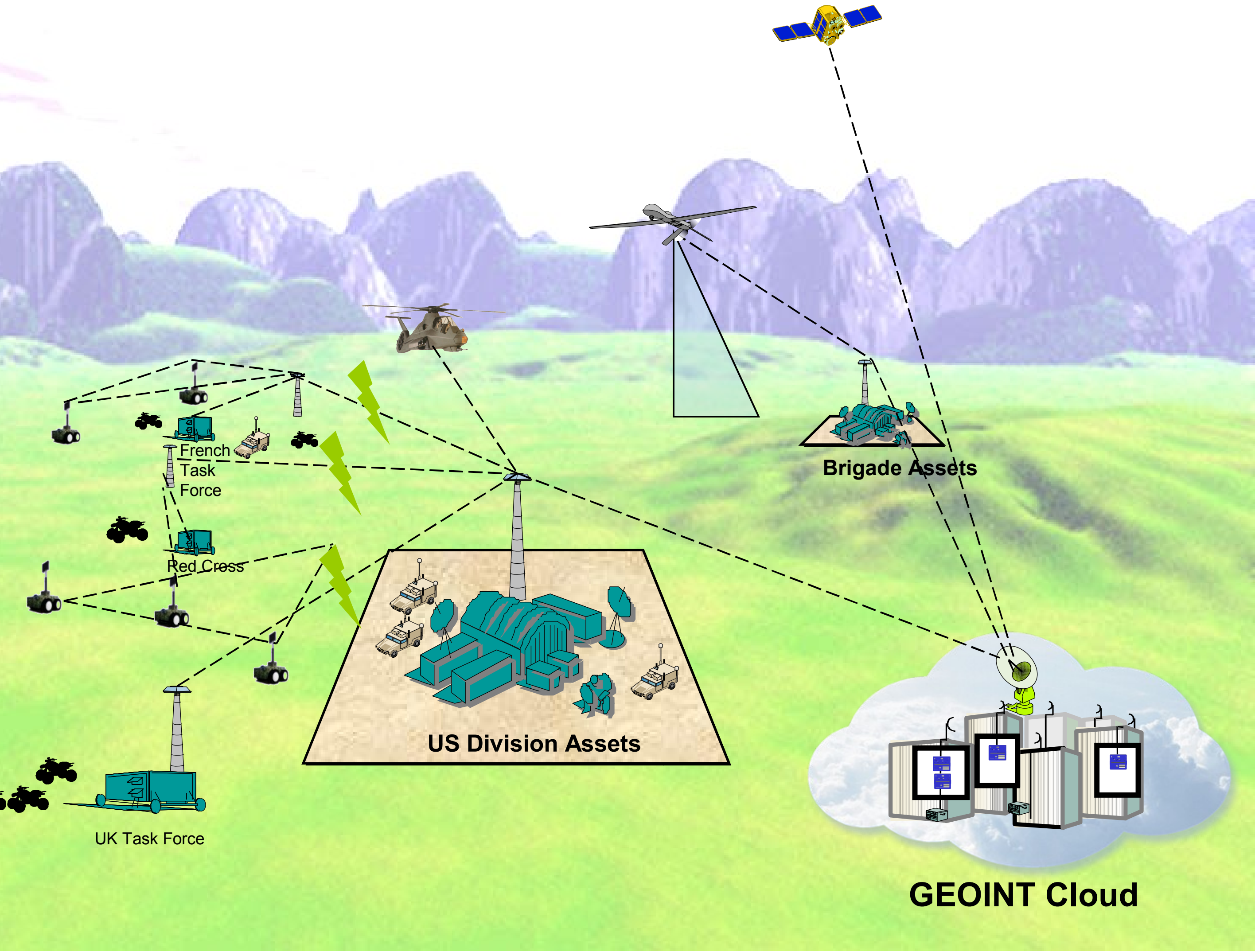
- **How do we maintain GEOINT data consistency and interoperability while maintaining application backward compatibility through as many as three versions?**

- **How do we provide electronic data mobility capable of supporting operational collaboration across the GEOINT community?**

GEOINT Cloud OV-1

GEOINT Cloud

- Self-service, on-demand capabilities
- Cloud delivered Exploitation Tools
- Multi-tenant GEOINT Data
- Elastic scalability
- Workload Mobility



Operational Concept

Self-Service Portal

Service Catalog
- GEOINT App
- GEOINT App
- GEOINT App

OPS Concept

- Self-service GEOINT Catalog
- Exploitation tools separated from data
- Move tools to data not data to tools
- Cloud multi-tenant security design

GEOINT Exploitation Virtual Machine

Hardware Software US Only VLAN

GEOINT Exploitation Virtual Machine

Hardware Software Coalition VLAN

Common Cloud Management Platform

Scheduling Workflow Provisioning Image Repository Monitoring Metering Migration

People and Identity

Privileged User Access
(centralized access and audit policies, directories)

Federated Identity Management
(single sign-on, identity provisioning technologies)

Privileged Account Management
(change control processes for privileged users)

Data and Information

Data Segregation
(encryption, network segmentation, Hardware / OS / App / Database isolation)

Data Recovery
(centralized backups, remote storage)

Data Redaction and Termination
(secure removal processes for customer data and metadata)

Data Leakage Prevention
(DLP technologies for data in motion and data at rest)

Application and Process

Compliance and Auditing
(audit policy creation, log generation and management)

Investigative Support
(audit retention, search, and correlation)

Policy Management
(unified security, governance, and policy enforcement)

Secure Provisioning
(image management, hardening, cohabitation policies)

Application Testing
(vulnerability assessment, fuzzing, app scanning, automated code reviews)

Network, Server, and Endpoint

Server Security
(trusted computing, auditing, access control)

Network Security
(Firewall, IPS, VLAN)

Virtualization Security
(VM Segmentation, Virtual Appliances, Integrated Hypervisor Security)

Browser Security
(ssl, memory protection, multi-level security, anti-malware)

Patch Management
(assessment, prioritization, scheduling, and application)

Physical Infrastructure

Data Location
(cloud data centers)

Disaster Recovery
(highly resilient clouds)

Cloud Availability
(multiple cloud centers)

GEOINT Data (US Only)

GEOINT Data (Coalition)

GEOINT Data (Civilian)

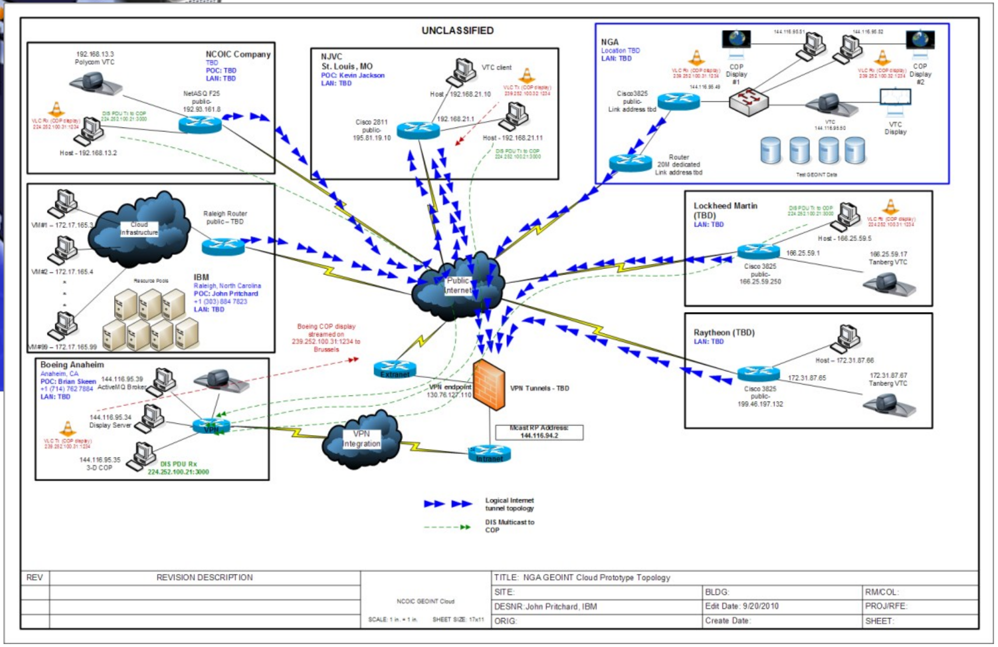
Operational Challenges

- **“Federated” Ownership & Governance of cloud deployment**
  - Which country should be used to run the cloud? Can it just be a single country or is there a distributed deployment of the cloud service required ?
- **Bandwidth**
  - How much bandwidth will be required for proper communication between end points in the battlefield and the cloud providing the “situational awareness” service?
- **Latency**
  - “Real-time” behavior is required for situational awareness service. Can this be achieved with a centralized cloud potentially sitting 1000’s of kilometers away from the troops?
- **Availability**
  - There are very high requirements against the continuous availability of the situational awareness as it provides information to troops in the battlefield about enemy position and position of friendly troops.
- **Security**
  - Success or failure in the battlefield can be influenced by the situational awareness cloud service. Therefore it is an ideal target for hackers. What are the security means to establish?

GEOINT Hybrid Cloud Experiment
Implementing the NCOIC Lab Interoperability Patotern

Cloud Experiments

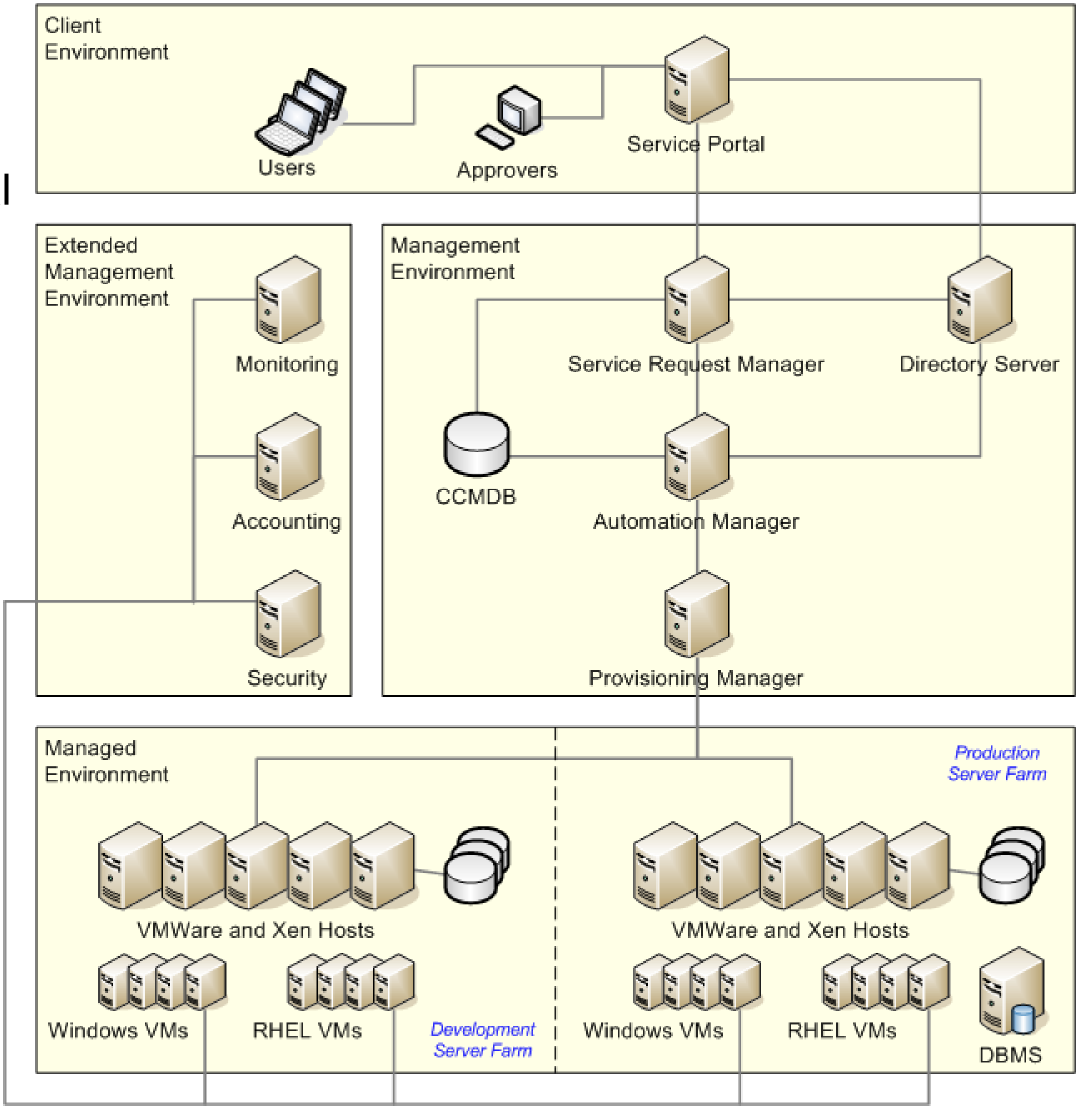
- #1 Physical Servers running Data Interoperability Middleware were migrated to Virtual Servers in the Cloud
- #2 Network Management capabilities delivered as a Cloud Service



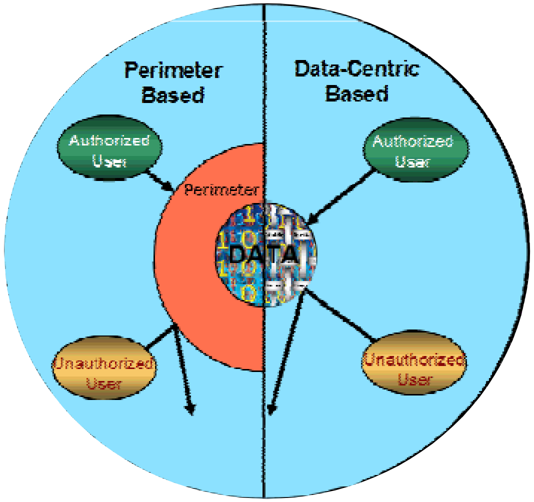
REV	REVISION DESCRIPTION		TITLE: NGA GEOINT Cloud Prototype Topology		
		NCOIC GEOINT Cloud	SITE:	BLDG:	RM/COL:
			DESNR: John Pritchard, IBM	Edit Date: 9/20/2010	PROJ/RFE:
		SCALE: 1 in. = 1 in. SHEET SIZE: 17x11	ORIG:	Create Date:	SHEET:

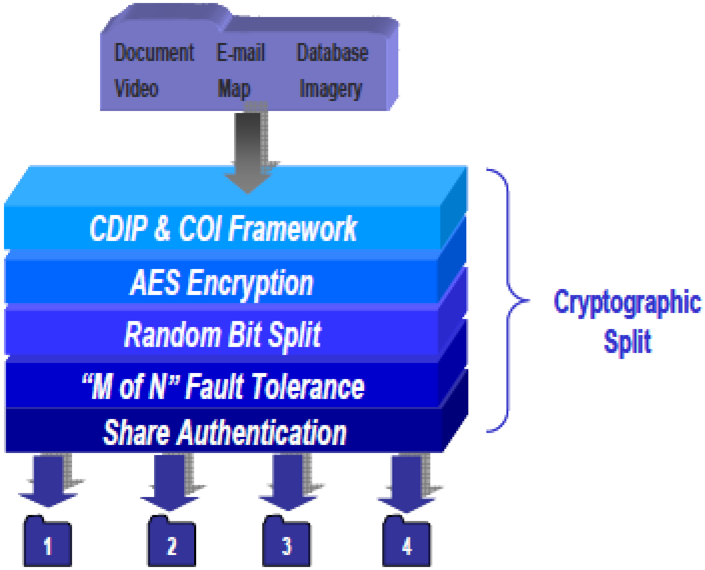
Prototype Operational Model

- Four Zones
  - Client Zone: Self-service Portal
  - Management Zone: Scheduling, Worklflow, Provisioning, Identity and Access
  - Extended Mgt Zone: Monitoring, Metering and Security
  - Managed Zone: Hypervisor Hosts
  - Each Zone can be co-located or geographically dispersed



Cryptographic Data Splitting





- Operates on arbitrary input data streams.
- Cross Domain Information Protection capabilities are integrated into the data.
- Internal AES encryption or an external encryption algorithm is used to protect the confidentiality of the data
- A random bit split is performed and the resulting bits are further physically separated into Shares further protecting the confidentiality of the data.
- M of N Fault Tolerance is added to provide a High Availability component where only M of the N Shares needs to be retrieved for reconstitution of the data.
- Each Share carries integrity (Trust) checks for itself and the other Shares.
- Physically separated data is outputted.
- NSA certified

Prototype Use Case (Draft)

- Data Access Policy
  - User 1 manages Red COI. User 1 can unilaterally revoke access to Red COI data.
  - Users 2 & 4 manage Green COI jointly. Joint approval required for access to Green COI data.
  - User 3 manages Blue COI. Access to Blue COI data only requires GEOINT cloud access.
- “Virtual Organization” Implementation – role-based authorization implemented using SAML and XACML
- Operational Tests
  - Coalition forms. All users have access to all data
  - User 1 unilaterally revokes Red COI data access
  - User 1 reinstates Red COI data access
  - User 2 unilaterally revokes Green COI data access
  - User 2 reinstates Green COI data access. User 4 revokes Green COI data access
  - User 4 reinstates Green COI data access
  - Coalition dissolves

OGC Resources
NCOIC Cloud Computing

- 30+ Implementation **Standards**
  - Geospatial / location Interoperability
  - Freely available, and widely implemented in the global marketplace
  - Implemented broadly worldwide
- **Process** - Over 40 Testbeds conducted to join industry and government to develop, test, validate and demonstrate OGC and complimentary web services standards / architectures.
- **Joint standards development and architecture best practice** testbed activities with Open Grid Forum, OASIS, IETF, IEEE and others
- **User Scenarios –** Defense, intelligence, homeland security scenarios employed in the planning and conduct of OGC activities
- **Access to** 400+ OGC industry, government, academic and research member organizations

Approved OGC Implementation Standards

Freely available at www.opengeospatial.org

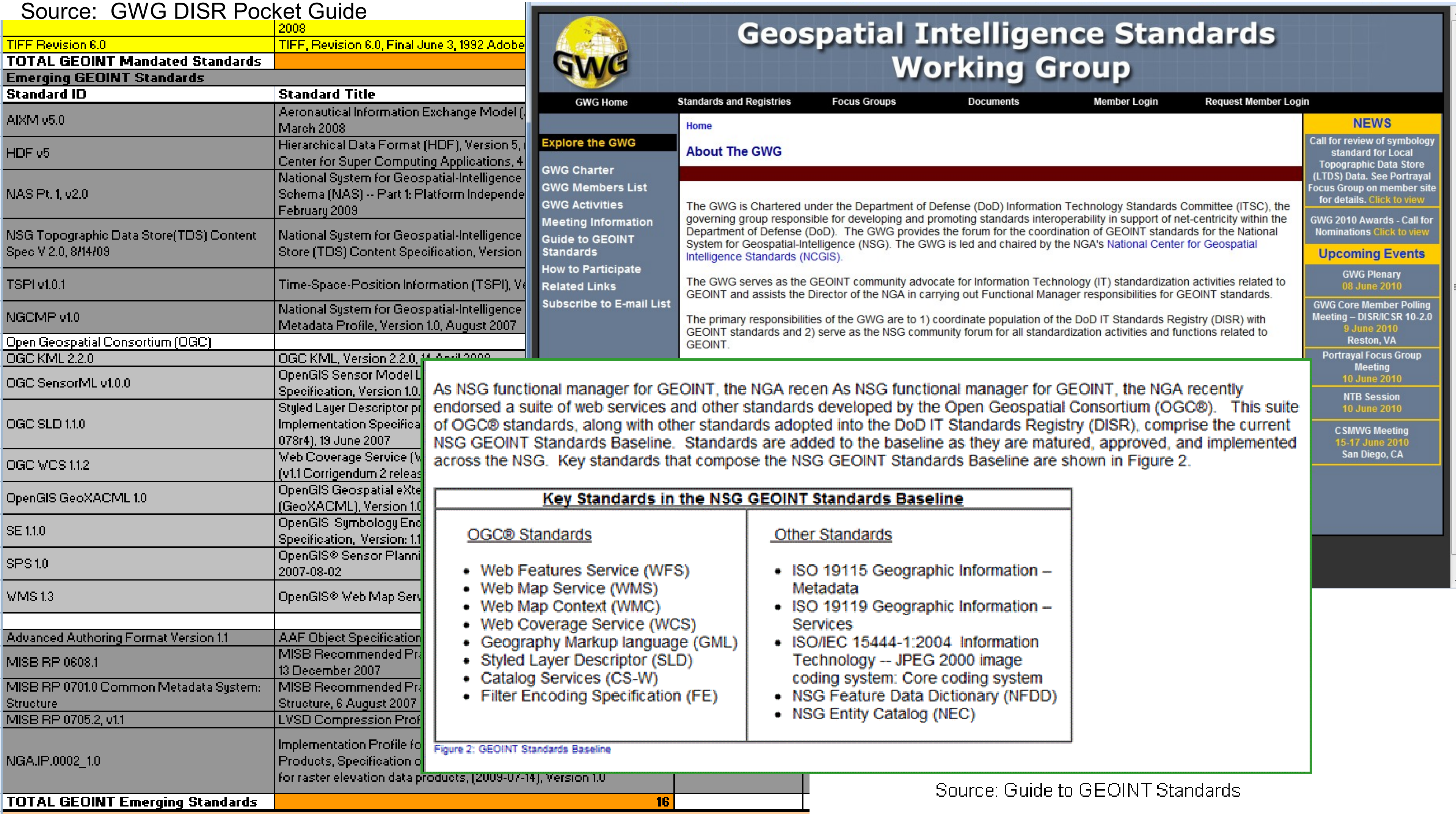
- **Catalogue Services**
  - Catalogue Service
- **Processing Services**
  - Open Location Services (OpenLS)
  - Coordinate Transformation Service
  - Sensor Planning Service (SPS)
  - Web Processing Service (WPS)
- **Portrayal Services**
  - Web Map Service
- **Data Services**
  - Grid Coverage Service
  - Simple Features (4)
  - Web Coverage Service
  - Web Feature Service

- **Encodings**
  - Geography Markup Language (GML)
  - Styled Layer Descriptor (SLD)
  - Transducer Markup Language (TML)
  - Sensor Model Language (SensorML)
  - CityGML
  - Web Map Context (WMC)
  - Observations & Measurements (O&M)
  - Filter Encoding
  - KML
  - Symbology Encoding
  - GML in JPEG 2000
  - Geographic Objects
  - GeoXACML
- **Web Services Common**
- **Open Location Services**

Geospatial Intelligence Standards Working Group
DOD IT Standards Registry

www.gwg.nga.mil

Source: GWG DISR Pocket Guide



	2008
TIFF Revision 6.0	TIFF, Revision 6.0, Final June 3, 1992 Adobe
TOTAL GEOINT Mandated Standards	
Emerging GEOINT Standards	
Standard ID	**Standard Title**
AIXM v5.0	Aeronautical Information Exchange Model (March 2008
HDF v5	Hierarchical Data Format (HDF), Version 5, (Center for Super Computing Applications, 4
NAS Pt. 1, v2.0	National System for Geospatial-Intelligence Schema (NAS) -- Part 1: Platform Independe February 2009
NSG Topographic Data Store(TDS) Content Spec V 2.0, 8/14/09	National System for Geospatial-Intelligence Store (TDS) Content Specification, Version
TSPI v1.0.1	Time-Space-Position Information (TSPI), Ve
NGCMP v1.0	National System for Geospatial-Intelligence Metadata Profile, Version 1.0, August 2007
Open Geospatial Consortium (OGC)	
OGC KML 2.2.0	OGC KML, Version 2.2.0, 14 April 2008
OGC SensorML v1.0.0	OpenGIS Sensor Model L Specification, Version 1.0.
OGC SLD 1.1.0	Styled Layer Descriptor pr Implementation Specifica 078r4), 19 June 2007
OGC WCS 1.1.2	Web Coverage Service (W (v1.1 Corrigendum 2 releas
OpenGIS GeoXACML 1.0	OpenGIS Geospatial eXte (GeoXACML), Version 1.0
SE 1.1.0	OpenGIS Symbology Enc Specification, Version: 1.1
SPS 1.0	OpenGIS® Sensor Planni 2007-08-02
WMS 1.3	OpenGIS® Web Map Serv
Advanced Authoring Format Version 1.1	AAF Object Specification
MISB RP 0608.1	MISB Recommended Pra 13 December 2007
MISB RP 0701.0 Common Metadata System: Structure	MISB Recommended Pra Structure, 6 August 2007
MISB RP 0705.2, v1.1	LVSD Compression Prof
NGA.IP.0002_1.0	Implementation Profile fo Products, Specification o for raster elevation data products, (2009-07-14), Version 1.0
TOTAL GEOINT Emerging Standards	16

GWG

Geospatial Intelligence Standards Working Group

GWG Home | Standards and Registries | Focus Groups | Documents | Member Login | Request Member Login

Explore the GWG

- GWG Charter
- GWG Members List
- GWG Activities
- Meeting Information
- Guide to GEOINT Standards
- How to Participate
- Related Links
- Subscribe to E-mail List

Home

About The GWG

The GWG is Chartered under the Department of Defense (DoD) Information Technology Standards Committee (ITSC), the governing group responsible for developing and promoting standards interoperability in support of net-centricity within the Department of Defense (DoD). The GWG provides the forum for the coordination of GEOINT standards for the National System for Geospatial-Intelligence (NSG). The GWG is led and chaired by the NGA's National Center for Geospatial Intelligence Standards (NCGIS).

The GWG serves as the GEOINT community advocate for Information Technology (IT) standardization activities related to GEOINT and assists the Director of the NGA in carrying out Functional Manager responsibilities for GEOINT standards.

The primary responsibilities of the GWG are to 1) coordinate population of the DoD IT Standards Registry (DISR) with GEOINT standards and 2) serve as the NSG community forum for all standardization activities and functions related to GEOINT.

NEWS

Call for review of symbology standard for Local Topographic Data Store (LTDS) Data. See Portrayal Focus Group on member site for details. Click to view

GWG 2010 Awards - Call for Nominations Click to view

Upcoming Events

GWG Plenary
08 June 2010

GWG Core Member Polling Meeting – DISR/ICSR 10-2.0
9 June 2010
Reston, VA

Portrayal Focus Group Meeting
10 June 2010

NTB Session
10 June 2010

CSMWG Meeting
15-17 June 2010
San Diego, CA

As NSG functional manager for GEOINT, the NGA recen As NSG functional manager for GEOINT, the NGA recently endorsed a suite of web services and other standards developed by the Open Geospatial Consortium (OGC®). This suite of OGC® standards, along with other standards adopted into the DoD IT Standards Registry (DISR), comprise the current NSG GEOINT Standards Baseline. Standards are added to the baseline as they are matured, approved, and implemented across the NSG. Key standards that compose the NSG GEOINT Standards Baseline are shown in Figure 2.

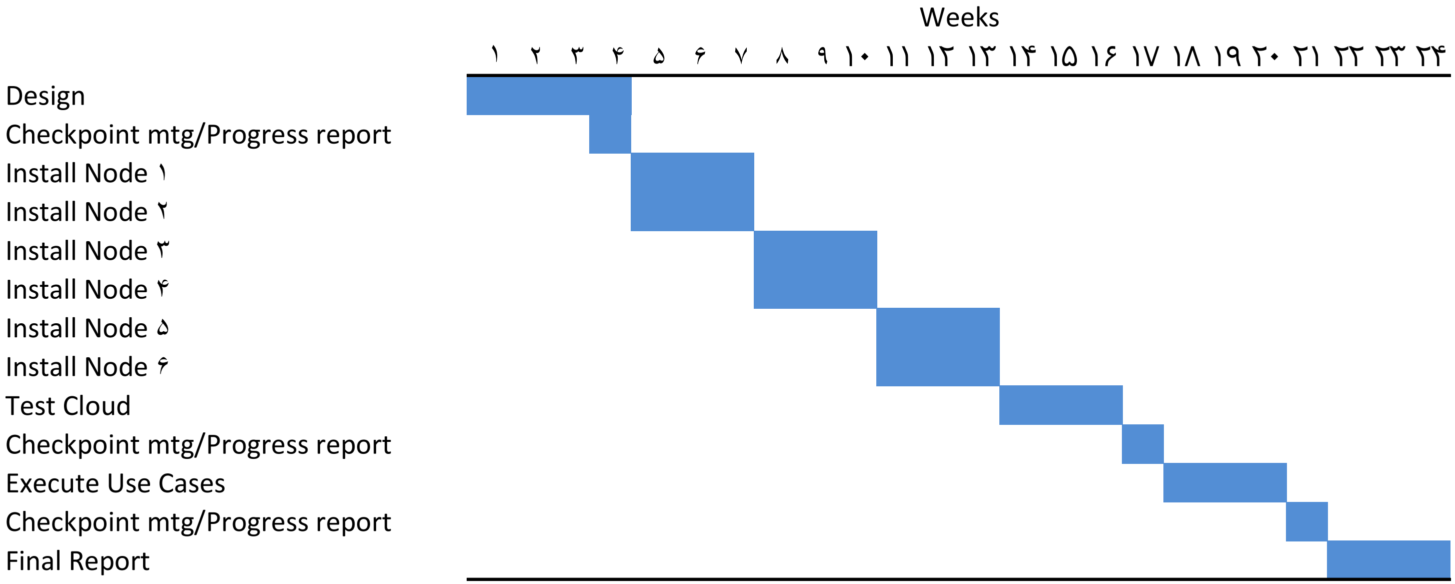
Key Standards in the NSG GEOINT Standards Baseline

OGC® Standards	Other Standards
• Web Features Service (WFS) • Web Map Service (WMS) • Web Map Context (WMC) • Web Coverage Service (WCS) • Geography Markup language (GML) • Styled Layer Descriptor (SLD) • Catalog Services (CS-W) • Filter Encoding Specification (FE)	• ISO 19115 Geographic Information – Metadata • ISO 19119 Geographic Information – Services • ISO/IEC 15444-1:2004 Information Technology -- JPEG 2000 image coding system: Core coding system • NSG Feature Data Dictionary (NFDD) • NSG Entity Catalog (NEC)

Figure 2: GEOINT Standards Baseline

Source: Guide to GEOINT Standards

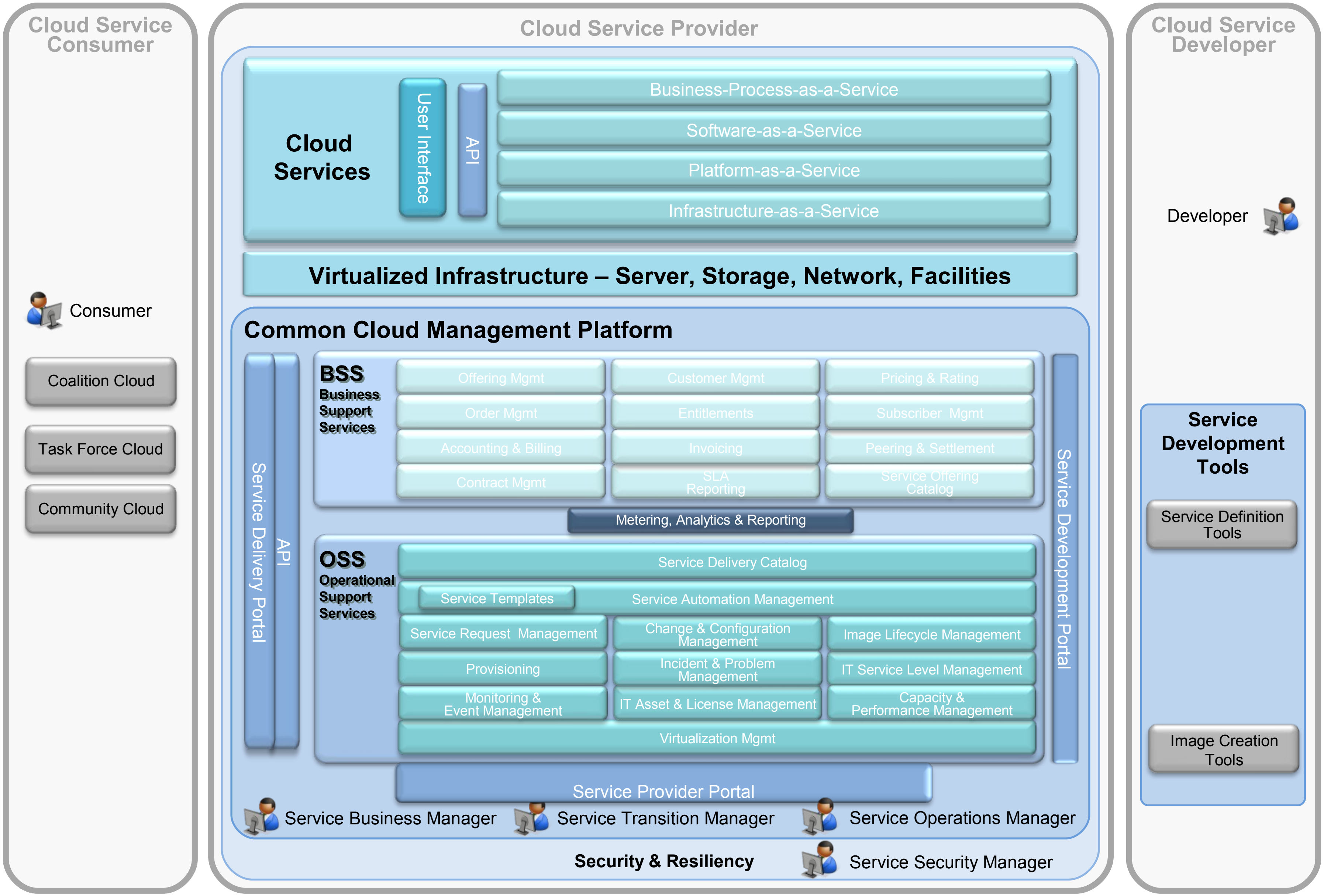
POA&M



- 2 FTE per node x 6 Nodes x 24 wks = 11520 hrs
- Skill Set
  - Cloud Architects
  - Network Engineers
  - Information Assurance SME
  - Cloud Consultants

Final use case definition required for proper scoping and sizing

Common Cloud Management Platform



Cloud Service Consumer

Consumer

Coalition Cloud

Task Force Cloud

Community Cloud

Cloud Service Provider

Cloud Services

User Interface

API

Business-Process-as-a-Service

Software-as-a-Service

Platform-as-a-Service

Infrastructure-as-a-Service

Virtualized Infrastructure – Server, Storage, Network, Facilities

Common Cloud Management Platform

Service Delivery Portal

API

BSS
Business Support Services

Offering Mgmt

Customer Mgmt

Pricing & Rating

Order Mgmt

Entitlements

Subscriber Mgmt

Accounting & Billing

Invoicing

Peering & Settlement

Contract Mgmt

SLA Reporting

Service Offering Catalog

Metering, Analytics & Reporting

OSS
Operational Support Services

Service Delivery Catalog

Service Templates

Service Automation Management

Service Request Management

Change & Configuration Management

Image Lifecycle Management

Provisioning

Incident & Problem Management

IT Service Level Management

Monitoring & Event Management

IT Asset & License Management

Capacity & Performance Management

Virtualization Mgmt

Service Development Portal

Service Provider Portal

Service Business Manager

Service Transition Manager

Service Operations Manager

Security & Resiliency

Service Security Manager

Cloud Service Developer

Developer

Service Development Tools

Service Definition Tools

Image Creation Tools

Architecture Decisions #1

- **Cloud Management Platform**
  - Where will the CMP be installed – physical/virtual machine type & OS ?
  - How many CMP’s will be installed (dev / test / prod / multi-site) ?
  - What specification for CMP platform (mem / cpu / disc) ?
  - What topology will be used to deploy the CMP (single, distributed, multi-tier) ?

- **Virtualised Infrastructure**
  - What hypervisor will be used?
  - Where are the components of the managed virtual infrastructure placed?
  - What is the capacity of the managed virtual infrastructure (dedicated to CMP)?
  - How are the physical server pools organized (shared / dedicated / resource specific)?

- **Network Infrastructure**
  - Which network zone will the CMP be placed?
  - Which network IP allocation schema will be used (range, pre-allocated, static, DHCP)?
  - How many virtual nics will be allocated to each virtual machine?
  - How are data/customer VLANs are allocated?
  - How are management VLANs allocated?

Architecture Decisions #2

- **Storage Infrastructure**
  - What storage (type/technology) will be allocated to the virtualized environment?
  - How are storage pools setup (for the virtualized environment)?
  - How is the storage structured for?
    - Image Data Store
    - Multiple VMs Data Stores
    - Backup Data Store
    - Separate data disk Data Store

- **Security**
  - What LDAP will be used for authentication / authorization / access control?
    - Integration with LDAP user directory for authentication of users and secure access to the self-service portal
    - Mapping of LDAP users and groups attributes to users, teams and roles
  - What, if any, special security software used in the management or managed environment?
  - Will the CMP have direct access to the virtualized environment or through firewalls?

Architecture Decisions #3

- **Availability**
  - Does CMP need high availability and what technology preferences exist?
  - What backup and restore technology should be used?
  - Does CMP need disaster recovery configuration and what technology preferences exist?

- **SLA**
  - What KPI´s are to be measured?
    - End to end service
    - Provisioning timeline

- **Sizing** (of the Managed environment and management systems)
  - Number of physical servers?
  - Number of virtual systems and size (CPU, memory disk) ?
  - Number of administrators ?
  - Number of end users ?
  - Frequency of provisioning requests (number of provisions per hr) ?
  - Rate of growth of traffic?

Architecture Decisions #4

- **Image management**
  - How many images will be required?
  - What is the initial catalog of images in image library?
  - What approach will be used for SW images (silent install, golden masters, etc) ?
  - What additional post-installation configuration is required (management, backup)?
  - Configuration of customer specific settings:
    - language, keyboard, time zone, etc.
    - Management components settings
    - Security settings

- **Usage and accounting**
  - What metrics will need to be metered and reported?
  - What variable / fixed pricing models will be used?
  - How will these metrics be mapped to chargeable accounts?

Architecture Decisions #5

- **Management of cloud services**
  - What SMTP server will be used for notifications?
  - How will the CMP be monitored and integrate with systems management?
  - What backup management will used for CMP & managed environment?
  - What change management is used?
  - What asset management is used?
  - What License management is used?

- **Multi-tenancy**
  - How are resources shared but servers separated (by VM, app, group, location, customer) ?
  - How are VLANs setup and allocated for multi-tenancy?

- **Presentation Layer**
  - What web browsers are supported in the organisation?
  - Will the CMP be delivered by an existing portal / presentation layer?
  - What level of presentation changes are required?